UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,539	03/02/2000	Simon Robert Walmsley	AUTH01US	4602

7590 02/07/2006

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain, 2041
AUSTRALIA

EXAMINER	
NGUYEN, NGA B	

ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 02/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/517,539	WALMSLEY ET AL.	
	Examiner	Art Unit	
	Nga B. Nguyen	3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is the answer to the Amendment filed on October 28, 2005, which paper has been placed of record in the file.

2. Claims 1-12 are pending in this application.

Response to Arguments/Amendment

3. Applicant's arguments with respect to claims 1-12 have been fully considered but are not persuasive.

In response to applicant's arguments that a skilled person in the art would not be motivated to combine Shigenaga with Lee, examiner respectfully submits that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Shigenaga does not disclose applying, in the untrusted authentication chip, a key one way function to the second decrypted outcome using the second secret key to produce an encrypted outcome. In Shigenaga, the IC card 2 sends the decryption data to the card terminal 1, the IC card 2 does not encrypt the decryption data using the private key before sending to the card terminal 1, thus card terminal 1 does not decrypt the encrypted data using the public key. Thus, the IC card 2 only performs decrypt function using the private key, the terminal card 1 only performs

encrypt function using the public key. However, Lee discloses the IC card performs both encrypt and decrypt function using an internal key stored in the card and the terminal card performs both encrypt and decrypt function using an identifying key stored in memory (column 6, lines 37-67). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to modify Shigenaga's to adopt the teaching of Lee for the purpose of improving the security, because the IC card 2 can apply the encrypt function using a secret key to encrypt the decryption data before sending to the card terminal 1, the card terminal 1 can apply the decrypt function using the public key to decrypt the encrypted data, thus the communication from the IC card 2 to the card terminal 1 is more secure with the encrypted data.

In conclusion, for the reason set forth above, examiner decides to maintain to previous rejection (also see details below) and make this Office action FINAL.

4. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 2, 4, 6, 7, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shigenaga, U.S. Patent No. 4,710,613, in view of Lee, U.S. Patent No. 5,923,759.

Regarding to claim 1, Shigenaga discloses a validation protocol for determining whether an untrusted authentication chip (column 6, lines 1-53, IC card 2 is equivalent to the untrusted authentication chip) is valid, or not, including the steps of:

generating a random number in a trusted authentication chip (column 7, lines 45-48; a random number is generated from random number data generator 120 of card terminal 1, card terminal 1 is equivalent to a trusted authentication chip);

applying, in the trusted authentication chip, a keyed one way function to the random number using a first key from the trusted authentication chip to produce a first encrypted outcome (column 7, lines 59-60, the RSA encrypter 121 in the card terminal 1 encrypts the random number using public key code, the card terminal 1 is equivalent to the trusted authentication chip, RSA encryption is asymmetric encryption function);

applying, in the untrusted authentication chip, a keyed one way function to the random number using a second secret key from the untrusted authentication chip to

produce a second decrypted outcome (column 7, line 65-column 8, line 12; decrypting in the IC card 2 the encrypted random number by the RSA decrypter 263 using the private key code from the IC card 2);

comparing the first encrypted outcome and the second decrypted outcome, without knowledge of the first key or the second key, and in the event of a match considering the untrusted chip to be valid (column 8, lines 28-42, 63-66, the decrypted random number is compared with the original random number by the comparison unit 15, without knowledge of the private key code stored in the IC card 2);

otherwise considering the untrusted chip to be invalid (column 6, lines 50-51, 65-67).

Shigenaga does not disclose applying, in the untrusted authentication chip, a key one way function to the second decrypted outcome using the second secret key to produce an encrypted outcome. In Shigenaga, the IC card 2 sends the decryption data to the card terminal 1, the IC card 2 does not encrypt the decryption data using the private key before sending to the card terminal 1, thus card terminal 1 does not decrypt the encrypted data using the public key. Thus, the IC card 2 only performs decrypt function using the private key, the terminal card 1 only performs encrypt function using the public key. However, Lee discloses the IC card performs both encrypt and decrypt function using an internal key stored in the card and the terminal card performs both encrypt and decrypt function using an identifying key stored in memory (column 6, lines 37-67). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to modify Shigenaga's to adopt the teaching of Lee for the

purpose of improving the security, because the IC card 2 can apply the encrypt function using a secret key to encrypt the decryption data before sending to the card terminal 1, the card terminal 1 can apply the decrypt function using the public key to decrypt the encrypted data, thus the communication from the IC card 2 to the card terminal 1 is more secure with the encrypted data.

Regarding to claim 2, Shigenaga further discloses the first and second keys are kept secret (column 6, lines 40-46, the "internal key" stored in the card; column 6, lines 55-60, the identifying key stored in memory 126).

Regarding to claim 4, Shigenaga further discloses the keyed one-way function is a symmetric cryptograph, a random number sequence, or a message authentication code (column 7, lines 1-15).

Claims 6, 7, 11 have similar limitations found in claims 1, 2, 4 above, therefore, are rejected by the same rationale.

7. Claims 3 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shigenaga, U.S. Patent No. 4,710,613, in view Lee, U.S. Patent No. 5,923,759, and further in view of Abraham et al (hereinafter Abraham), U.S. Patent No. 4,799,061.

Regarding to claims 3 and 10, Shigenaga does not disclose the domain of the random numbers generated is non-deterministic. However, Abraham discloses the domain of the random numbers generated is non-deterministic (column 3, lines 9-13, the random numbers generated is non-deterministic because each challenge requires the use of a new random number). Therefore, it would have been obvious to modify Shigenaga's to adopt the teaching of Abraham above for the purpose of providing high

security level because each challenge requires a new random number, thus the unauthorized person cannot easily to predict the random number.

8. Claims 5, 8, 9, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shigenaga, U.S. Patent No. 4,710,613, in view Lee, U.S. Patent No. 5,923,759, and further in view of Thomlinson et al (herein after Thomlinson), U.S. Patent No. 5,778,069.

Regarding to claims 5 and 12, Shigenaga discloses the one-way function is a symmetric cryptographic function (column 7, lines 1-15), but Shigenaga does not disclose the key has a minimum size of 128 bits. However, Thomlinson discloses the key has a minimum size of 128 bits (column 5, lines 59-65). Therefore, it would have been obvious to modify Shigenaga's to adopt the teaching of Thomlinson above for the security purpose because producing the encryption and decryption keys with larger bits makes the unauthorized person cannot easily to guess the keys.

Regarding to claims 8 and 9, Shigenaga does not disclose the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed, and for a group of authentication chips, each chip has a different initial seed, so that the first call to each chip requesting a random number will produce different results for each chip in the group. However, Thomlinson discloses the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be

produced from a new seed (column 6, lines 36-60). Moreover, it is well known to use a different initial seed for each chip in the group of chip. Therefore, it would have been obvious to modify Lee's to adopt the teaching of Thomlinson above for the purpose of providing high security level because each random number is generated from a new seed and each chip has a different initial seed, thus the unauthorized person cannot easily to predict the random number.

Conclusion

9. Claims 1-12 are rejected.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner Nga B. Nguyen whose telephone number is (571) 272-6796. The examiner can normally be reached on Monday-Thursday from 9:00AM-6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung S. Sough can be reached on (571) 272-6799.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-3600.

11. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

C/o Technology Center 3600

Washington, DC 20231

Or faxed to:

(703) 872-9306 (for formal communication intended for entry),

or

(571) 273-0325 (for informal or draft communication, please label "PROPOSED" or "DRAFT").

Hand-delivered responses should be brought to Knox building, 501 Dulany Street, Alexandria, VA, First Floor (Receptionist).

Nga B. Nguyen
Nga Nguyen
January 5, 2006